

# AN IMPROVEMENT TO AN ALGORITHM OF BELABAS, DIAZ Y DIAZ AND FRIEDMAN

LOÏC GRENIÉ AND GIUSEPPE MOLTENI

ABSTRACT. In [BDF08] Belabas, Diaz y Diaz and Friedman show a way to determine, assuming the Generalized Riemann Hypothesis, a set of prime ideals that generate the class group of a number field. Their method is efficient because it produces a set of ideals that is smaller than earlier proved results. Here we show how to use their main result to algorithmically produce a bound that is lower than the one they prove.

## 1. INTRODUCTION

We refer the reader to the paper [BDF08] for an outline of Buchmann's algorithm.

Let  $\mathbf{K}$  be a number field of degree  $n_{\mathbf{K}}$ , with  $r_1$  (resp.  $r_2$ ) real (resp. pair of complex) embeddings. We denote  $\Delta_{\mathbf{K}}$  the absolute value of its discriminant.

**Definition 1.** Let  $\mathcal{W}$  be the set of functions  $F: [0, +\infty) \rightarrow \mathbf{R}$  such that

- $F$  is continuous;
- $\exists \varepsilon > 0$  such that the function  $F(x)e^{(\frac{1}{2}+\varepsilon)x}$  is integrable and of bounded variation;
- $F(0) > 0$ ;
- $(F(0) - F(x))/x$  is of bounded variation.

Let then, for  $T > 1$ ,  $\mathcal{W}(T)$  be the subset of  $\mathcal{W}$  such that

- $F$  has support in  $[0, \log T]$ ;
- the Fourier cosine transform of  $F$  is non-negative.

The main result of [BDF08] is, up to a minor reformulation:

**Theorem 2 (Belabas, Diaz y Diaz, Friedman).** Let  $\mathbf{K}$  be a number field satisfying the Riemann Hypothesis for all L-functions attached to non-trivial characters of its ideal class group  $\mathcal{C}_{\mathbf{K}}$ , and suppose there exists, for some  $T > 1$ , an  $F \in \mathcal{W}(T)$  with  $F(0) = 1$  and such that

$$(3) \quad 2 \sum_{\mathfrak{p}} \log \mathrm{N}\mathfrak{p} \sum_{m=1}^{+\infty} \frac{F(m \log \mathrm{N}\mathfrak{p})}{\mathrm{N}\mathfrak{p}^{m/2}} > \log \Delta_{\mathbf{K}} - n_{\mathbf{K}} \gamma - n_{\mathbf{K}} \log(8\pi) - \frac{r_1 \pi}{2} \\ + r_1 \int_0^{+\infty} \frac{1 - F(x)}{2 \cosh(x/2)} dx + n_{\mathbf{K}} \int_0^{+\infty} \frac{1 - F(x)}{2 \sinh(x/2)} dx .$$

Then the ideal class group of  $\mathbf{K}$  is generated by the prime ideals of  $\mathbf{K}$  having norm less than  $T$ .

The authors apply the result to the function  $\frac{1}{L} C_L * C_L$  where  $L = \log T$ ,  $*$  is the convolution operator and  $C_L$  is the characteristic function of  $(-\frac{L}{2}, \frac{L}{2})$ , to get the

---

2010 *Mathematics Subject Classification.* Primary 11R04; Secondary 11R29.

**Corollary 4 (Belabas, Diaz y Diaz, Friedman).** *Suppose  $\mathbf{K}$  is a number field satisfying the Riemann Hypothesis for all L-functions attached to non-trivial characters of its ideal class group  $\mathcal{C}_{\mathbf{K}}$ , and for some  $T > 1$  we have*

$$(5) \quad 2 \sum_{\substack{\mathfrak{p}, m \\ N\mathfrak{p}^m < T}} \frac{\log N\mathfrak{p}}{N\mathfrak{p}^{m/2}} \left( 1 - \frac{\log N\mathfrak{p}^m}{\log T} \right) > \log \Delta_{\mathbf{K}} - n_{\mathbf{K}} \left( \gamma + \log(8\pi) - \frac{c_1}{\log T} \right) \\ - r_1 \left( \frac{\pi}{2} - \frac{c_2}{\log T} \right),$$

where

$$c_1 = \frac{\pi^2}{2}, \quad c_2 = 4C.$$

(Here  $C = \sum_{k \geq 0} (-1)^k (2k+1)^{-2} = 0.915965 \dots$  is Catalan's constant.)

Then the ideal class group of  $\mathbf{K}$  is generated by the prime ideals of  $\mathbf{K}$  having norm less than  $T$ .

Our aim is to find a good  $T$  for the number field  $\mathbf{K}$  as fast as possible exploiting the bilinearity of the convolution product.

## 2. SETUP

We use the following definition to simplify a little bit the language.

**Definition 6.** A bound for  $\mathbf{K}$  is an  $L = \log T$  with  $T$  as in Theorem 2.

**2.1. Rewriting the theorem.** We begin by homogenizing Equation (3) and relaxing the requirement  $F(0) = 1$  to  $F(0) > 0$  so that now the condition on the function is

$$(7) \quad 2 \sum_{\mathfrak{p}} \log N\mathfrak{p} \sum_{m=1}^{+\infty} \frac{F(m \log N\mathfrak{p})}{N\mathfrak{p}^{m/2}} > F(0) \left( \log \Delta_{\mathbf{K}} - n_{\mathbf{K}} \gamma - n_{\mathbf{K}} \log(8\pi) - \frac{r_1 \pi}{2} \right) \\ + r_1 \int_0^{+\infty} \frac{F(0) - F(x)}{2 \cosh(x/2)} dx + n_{\mathbf{K}} \int_0^{+\infty} \frac{F(0) - F(x)}{2 \sinh(x/2)} dx.$$

**Definition 8.** Let  $\mathcal{S}$  be the real vector space of even and compactly supported step functions and, for  $T > 1$ , let  $\mathcal{S}(T)$  be the subspace of  $\mathcal{S}$  of functions supported in  $\left[ -\frac{\log T}{2}, \frac{\log T}{2} \right]$ .

**Definition 9.** For any integer  $N \geq 1$  and positive real  $\delta$  we define the subspace  $\mathcal{S}(N, \delta)$  of  $\mathcal{S}(e^{2N\delta})$  made of functions which are constant  $\forall k \in \mathbf{N}$  on  $[k\delta, (k+1)\delta)$ .

The elements of  $\mathcal{S}(N, \delta)$  are thus step functions with fixed step width  $\delta$ . If  $N \geq 1$ ,  $\delta > 0$  and  $T = e^{2N\delta}$  we have

$$(10a) \quad \mathcal{S}(N, \delta) \subset \mathcal{S}(T) \subset \mathcal{S}$$

$$(10b) \quad \forall \Phi \in \mathcal{S}(T), \quad \frac{1}{\|\Phi\|_2^2} \Phi * \Phi \in \mathcal{W}(T)$$

$$(10c) \quad \mathcal{S}(N, \delta) \subset \mathcal{S}(N+1, \delta)$$

$$(10d) \quad \forall k \geq 1, \quad \mathcal{S}\left(kN, \frac{\delta}{k}\right) \subseteq \mathcal{S}(N, \delta).$$

If, for some  $T > 1$ ,  $\Phi \in \mathcal{S}(T)$  and  $F = \Phi * \Phi$  satisfies (7) then, according to Theorem 2,  $\mathcal{C}_{\mathbf{K}}$  is generated by prime ideals  $\mathfrak{p}$  such that  $N\mathfrak{p} < T$ . This leads us to define the linear form  $\ell_{\mathbf{K}}$  on  $\mathcal{S} * \mathcal{S}$  by

$$\begin{aligned} \ell_{\mathbf{K}}(F) = -2 \sum_{\mathfrak{p}} \log N\mathfrak{p} \sum_{m=1}^{+\infty} \frac{F(m \log N\mathfrak{p})}{N\mathfrak{p}^{m/2}} + F(0) \left( \log \Delta_{\mathbf{K}} - n_{\mathbf{K}}\gamma - n_{\mathbf{K}} \log(8\pi) - \frac{r_1\pi}{2} \right) \\ + r_1 \int_0^{+\infty} \frac{F(0) - F(x)}{2 \cosh(x/2)} dx + n_{\mathbf{K}} \int_0^{+\infty} \frac{F(0) - F(x)}{2 \sinh(x/2)} dx \end{aligned}$$

and the quadratic form  $q_{\mathbf{K}}$  on  $\mathcal{S}$  by  $q_{\mathbf{K}}(\Phi) = \ell_{\mathbf{K}}(\Phi * \Phi)$ . We can at this point give a weaker version of Theorem 2 as

**Corollary 11.** *Let  $\mathbf{K}$  be a number field satisfying GRH and  $T > 1$ . If the restriction of  $q_{\mathbf{K}}$  to  $\mathcal{S}(T)$  has a negative eigenvalue then  $\mathcal{C}_{\mathbf{K}}$  is generated by prime ideals  $\mathfrak{p}$  such that  $N\mathfrak{p} < T$ .*

Note that  $q_{\mathbf{K}}$  is a continuous function as a function from  $(\mathcal{S}(T), \|\cdot\|_1)$  to  $\mathbf{R}$ . Therefore if  $\log T$  is a bound for  $\mathbf{K}$  then there exists an  $L' < \log T$  such that  $L'$  is a bound for  $\mathbf{K}$ . Note also that, in terms of  $T$ , only the norms of prime ideals are relevant, which means that we do not need the smallest possible  $T$  to get the best result.

*Remark.* If  $T > 1$  and  $\Phi \in \mathcal{S}(T)$ , then for any  $\varepsilon > 0$  there exists  $N \geq 1$ ,  $\delta > 0$  and  $\Phi_{\delta} \in \mathcal{S}(N, \delta)$  such that  $\|\Phi * \Phi - \Phi_{\delta} * \Phi_{\delta}\|_{\infty} \leq \varepsilon$  and  $e^{2N\delta} \leq T$ . Hence we do not lose anything in terms of bounds if we consider only the subspaces of the form  $\mathcal{S}(N, \delta)$ .

**2.2. Computing the integrals.** Let  $T > 1$  be a real,  $L = \log T$  and  $F_L = C_L * C_L$  where, as above,  $C_L$  is the characteristic function of  $[-\frac{L}{2}, \frac{L}{2}]$ . We readily see that  $F_L(x) = (L-x)C_{2L}(x)$  for any  $x \geq 0$ . We easily compute

$$\int_0^{+\infty} \frac{F_L(0) - F_L(x)}{2 \cosh(x/2)} dx = 4C - 4 \operatorname{Im} \operatorname{dilog} \left( \frac{i}{\sqrt{T}} \right)$$

and

$$\int_0^{+\infty} \frac{F_L(0) - F_L(x)}{2 \sinh(x/2)} dx = \frac{\pi^2}{2} - 4 \operatorname{dilog} \left( \frac{1}{\sqrt{T}} \right) + \operatorname{dilog} \left( \frac{1}{T} \right)$$

where  $C$  is Catalan's constant and  $\operatorname{dilog}(x)$  is the dilogarithm function normalized to be the primitive of  $-\frac{\log(1-x)}{x}$  such that  $\operatorname{dilog}(0) = 0$  (this is the normalization of [PARI15]).

**2.3. A remark on the restriction of quadratic forms.** Let  $q$  be a quadratic form on an  $n$ -dimensional vector space  $V$  of signature  $(z, p, m)$ . We can interpret  $p$  (resp.  $m$ ) as the dimension of a maximal subspace on which  $q$  is positive (resp. negative) definite while the kernel of  $q$  has dimension  $z = n - p - m$ .

Let  $H$  be an hyperplane of  $V$  and  $q'$  the restriction of  $q$  to  $H$ . A maximal subspace on which  $q'$  is definite is a subspace on which  $q$  is definite, thus the intersection of a maximal subspace on which  $q$  is definite with  $H$ . This means the signature  $(z', p', m')$  of  $q'$  will be such that  $p' \leq p \leq p' + 1$  and  $m' \leq m \leq m' + 1$ . Cases  $p = p' + 1$ ,  $m = m' + 1$  and  $p = p'$ ,  $m = m'$  are both possible with  $z = n - p - m = z' - 1$  and  $z = z' + 1$  respectively.

## 3. IMPROVING THE RESULT

**3.1. Basic bound.** We restate [BDF08, Section 3, p. 1191] which determines an optimal bound for Corollary 4. Let  $\text{GRHcheck}(\mathbf{K}, \log T)$  be the function that returns the right hand side of (5) minus its left hand side and  $\text{BDyDF}(\mathbf{K})$  be the function which computes the optimal bound, by dichotomy for instance. The computation of  $\text{BDyDF}(\mathbf{K})$  is very fast because the only arithmetic information we need on  $\mathbf{K} \simeq \mathbf{Q}[x]/(P)$  is the splitting information for primes  $p < T$  and is determined easily for nearly all  $p$ . Indeed if  $p$  does not divide the index of  $\mathbf{Z}[x]/(P)$  in  $\mathcal{O}_K$ , then the splitting of  $p$  in  $\mathbf{K}$  is determined by the factorization of  $P \bmod p$ . We can also store such splitting information for all  $p$  that we consider and do not recompute it each time we test whether a given bound  $\log T$  is sufficient.

**3.2. Improving the bound.** We fix a number field  $\mathbf{K}$ . We denote  $q_{\mathbf{K}, N, \delta}$  the restriction of  $q_{\mathbf{K}}$  to  $\mathcal{S}(N, \delta)$ . According to Corollary 11, if  $q_{\mathbf{K}, N, \delta}$  has a negative eigenvalue then  $2N\delta$  is a bound for  $\mathbf{K}$ . This justifies the following definition.

**Definition 12.** *The pair  $(N, \delta)$  is  $K$ -good when  $q_{\mathbf{K}, N, \delta}$  has a negative eigenvalue.*

We can reinterpret Functions  $\text{GRHcheck}$  and  $\text{BDyDF}$  saying that if  $\text{GRHcheck}(\mathbf{K}, 2\delta)$  is negative then  $(1, \delta)$  is  $K$ -good and that  $(1, \frac{1}{2} \log \text{BDyDF}(\mathbf{K}))$  is  $K$ -good.

As a first step to improve on Corollary 4, given  $\delta > 0$  we look for the smallest  $N$  such that  $(N, \delta)$  is  $K$ -good. Looking for such an  $N$  can be done fairly easily with this setup. For any  $i \geq 1$ , let  $\Phi_i$  be the characteristic function of  $(-i\delta, i\delta)$ . Then  $(\Phi_i)_{1 \leq i \leq N}$  is a basis of  $\mathcal{S}(N, \delta)$ . We have  $\Phi_i * \Phi_i = F_{2i\delta} = (2i\delta - |x|)C_{4i\delta}(|x|)$ ; observe also that the function considered in Corollary 4 is  $\frac{1}{\log T} F_{\log T}$ . We further observe that

$$\Phi_i * \Phi_j = F_{(i+j)\delta} - F_{|i-j|\delta}.$$

This means that the matrix  $A_N$  of  $q_{\mathbf{K}, N, \delta}$  can be computed by computing only the values of  $\ell_{\mathbf{K}}(F_{2i\delta})$  for  $1 \leq i \leq 2N$  and subtracting those values.

We then stop when the determinant of  $A_N$  is negative or when  $2N\delta \geq \text{BDyDF}(\mathbf{K})$ . This does not guarantee that we stop as soon as there is a negative eigenvalue. Indeed, consider the following sequence of signatures:

$$(0, p, 0) \rightarrow (1, p, 0) \rightarrow (1, p, 1) \rightarrow (0, p+1, 2) \rightarrow \dots$$

We should have stopped when the signature was  $(1, p, 1)$  however the determinant was zero there. Our algorithm will stop as soon as there is an odd number of negative eigenvalues (and no zero) or we go above  $\text{BDyDF}(\mathbf{K})$ . Such unfavorable sequence of signatures is however very unlikely and can be ignored in practice.

The corresponding algorithm is presented in Function `NDelta`. We have added a limit  $N_{\max}$  for  $N$  which is not needed right now but will be used later. In Function `NDelta`, we need to slightly change  $\text{GRHcheck}$  to returns the difference of both sides of Equation (7) instead of (5). Note that  $(\Phi_i)$  is a basis adapted to the inclusion (10c) so that we only need to compute the edges of the matrix  $A_N$  at each step. The test  $\det A < 0$  in line 13 can be implemented using Cholesky  $LDL^*$  decomposition which is incremental.

One way to use this function is to compute  $T = \text{BDyDF}(\mathbf{K})$  and for some  $N_{\max} \geq 2$ , let  $\delta = \frac{\log T}{2N_{\max}}$  and  $N = \text{NDelta}(\mathbf{K}, \delta, N_{\max})$ . Using the inclusion (10d), we see that  $(N, \delta)$  is  $K$ -good and that  $N \leq N_{\max}$ , so that we have improved the bound.

**3.3. Adaptive steps.** Unfortunately Function **NDelta** is not very efficient mostly for two reasons. To explain them and to improve the function we introduce some extra notations. For any  $\delta > 0$ , let  $N_\delta$  be the minimal  $N$  such that  $(N, \delta)$  is  $K$ -good. Observe that Function **NDelta** computes  $N_\delta$ , as long as  $N_\delta \leq N_{\max}$  and no zero eigenvalue prevents success. Obviously, using (10c), we see that for any  $N \geq N_\delta$ ,  $(N, \delta)$  is  $K$ -good. We have observed numerically that the sequence  $N\delta_N$  is roughly decreasing, i.e. for most values of  $N$  we have  $N\delta_N \geq (N+1)\delta_{N+1}$ .

For any  $N \geq 1$ , let  $\delta_N$  be the infimum of the  $\delta$ 's such that  $(N, \delta)$  is  $K$ -good. It is not necessarily true that if  $\delta \geq \delta_N$  then  $(N, \delta)$  is  $K$ -good, however we have never found a counterexample. The function  $\delta \mapsto \delta N_\delta$  is piecewise linear with discontinuities at points where  $N_\delta$  changes; the function is increasing in the linear pieces and decreasing at the discontinuities. This means that if we take  $0 < \delta_2 < \delta_1$  but we have  $N_{\delta_2} > N_{\delta_1}$  then we may have  $N_{\delta_2}\delta_2 > N_{\delta_1}\delta_1$  so the bound we get for  $\delta_2$  is not necessarily as good as the one for  $\delta_1$ .

The resolution of Function **NDelta** is not very good: going from  $N-1$  to  $N$  the bound for the norm of the prime ideals is multiplied by  $e^{2\delta}$ . This is the first reason reducing the efficiency of the function. The second one is that if  $N_{\max}$  is above 20 or so, the number  $\delta = \frac{\log \text{BDyDF}(\mathbf{K})}{2N_{\max}}$  has no specific reason to be near  $\delta_{N_\delta}$ ; as discussed above, this means that we can get a better bound for  $\mathbf{K}$  by choosing  $\delta$  to be just above either  $\delta_{N_\delta}$  or  $\delta_{1+N_\delta}$ . Both reasons derive from the same facts and give a bound for  $\mathbf{K}$  that can be overestimated by at most  $2\delta$  for the considered  $N = \text{NDelta}(\mathbf{K}, \delta, N_{\max})$ .

To improve the result, we can use once again inclusion (10d) and determine a good approximation of  $\delta_N$  for  $N = 2^n$ . We determine first by dichotomy a  $\delta_0$  such that  $(N_0, \delta_0)$  is  $K$ -good for some  $N_0 \geq 1$  (we use  $N_0 = 8$  in our computation). For any  $k \geq 0$ , we take  $N_{k+1} = 2N_k$  and determine by dichotomy a  $\delta_{k+1}$  such that  $(N_{k+1}, \delta_{k+1})$  is  $K$ -good; we already know that  $\frac{\delta_k}{2}$  is an upper bound for  $\delta_{k+1}$  and we can either use 0 as a lower bound or try to find a lower bound not too far from the upper bound because the upper bound is probably not too bad. The algorithm is described in Function **Bound**. It uses a subfunction **OptimalT**( $\mathbf{K}, N, T_l, T_h$ ) which returns the smallest integer  $T \in [T_l, T_h]$  such that  $\text{NDelta}(\mathbf{K}, \log T/(2N), N) > 0$ . The algorithm does not return a bound below those proved in and .

**3.4. Further refinements.** To reduce the time used to compute the determinants, we tried to use steps of width  $4\delta$  in  $[-\frac{1}{2} \log T, \frac{1}{2} \log T]$  and of width  $2\delta$  in the rest of  $[-\frac{3}{4} \log T, \frac{3}{4} \log T]$ , to halve the dimension of  $\mathcal{S}(N, \delta)$ . It worked in the sense that we found substantially the same  $T$  faster. However we decided that the total time of the algorithm is not high enough to justify the increase in code complexity.

## 4. EXAMPLES

In this section we will denote  $T(\mathbf{K})$  the result of Function **BDyDF** and  $T_1(\mathbf{K})$  the result of Function **Bound**.

**4.1. Various fields.** We tested the algorithm on several fields. Let first  $\mathbf{K} = \mathbf{Q}[x]/(P)$  where

$$P = x^3 + 559752270111028720x + 55137512477462689.$$

The polynomial  $P$  has been chosen so that for all primes  $2 \leq p \leq 53$  there are two prime ideals of norms  $p$  and  $p^2$ . This ensures that there are lots of small norms of prime ideals. We have  $T(\mathbf{K}) = 19162$ . There are 2148 non-zero prime ideals with norms up to  $T(\mathbf{K})$ . We found that  $T_1(\mathbf{K}) = 11071$  and that there are 1343 non-zero prime ideals of norms up to  $T_1(\mathbf{K})$ .

The time used by Function **BDyDF** was 58ms on our test computer while the time used by our algorithm was an *additional* 36ms. The test was designed in such a way that our algorithm used the decomposition information of Function **BDyDF**, so it saved a little time.

We tested also the algorithm on the set of 4686 fields of degree 2 to 27 and small discriminant coming from a benchmark of [PARI15]. The mean value of  $\frac{T_1(\mathbf{K})}{T(\mathbf{K})}$  for those fields is lower than  $\frac{1}{2}$ .

For cyclotomic fields, the new algorithm does not give results significantly better than those of Belabas, Diaz y Diaz and Friedman. It might be because the discriminant of a cyclotomic field is not large enough with respect to its degree.

**4.2. Pure fields.** We computed  $T(\mathbf{K})$  and  $T_1(\mathbf{K})$  for fields of the form  $\mathbf{Q}[x]/(P)$  with  $P = x^n \pm p$  and  $p$  is the first prime after  $10^a$  for a certain family of integers  $n$  and  $a$ . We computed the family of  $\frac{T_1(\mathbf{K})}{T(\mathbf{K})}$  for each fixed degree. The graph shows that it is decreasing with the discriminant. The graph of  $\frac{T_1(\mathbf{K})}{T(\mathbf{K})}(\log \log \Delta_{\mathbf{K}})^2$  is much more regular and looks to have a non-zero limit, see Figure 1 below. We computed the mean of  $\frac{T_1(\mathbf{K})}{T(\mathbf{K})}(\log \log \Delta_{\mathbf{K}})^2$  for each fixed degree. The results are summarized below:

$P$	$a \leq$	$\log \Delta_{\mathbf{K}} \leq$	mean
$x^2 - p$	3999	9212	13.19
$x^6 + p$	1199	13818	13.38
$x^{21} - p$	328	15169	13.68

The small discriminants are (obviously) much less sensitive to the new algorithm. We reduced the range for each series to have  $\log \Delta_{\mathbf{K}} \leq 500$ . The results are as follows:

$P$	$a \leq$	mean
$x^2 - p$	218	12.35
$x^6 + p$	43	13.66
$x^{21} - p$	10	17.19

**4.3. Biquadratic fields.** We repeated the computations above also for biquadratic fields  $\mathbf{Q}[\sqrt{p_1}, \sqrt{p_2}]$  where each  $p_i$  is the first prime after  $10^{a_i}$  for a certain family of integers  $a_i$ . We found that the mean of  $\frac{T_1(\mathbf{K})}{T(\mathbf{K})}(\log \log \Delta_{\mathbf{K}})^2$  is 13.63 for the 7119 fields computed and 13.88 if we restrict the family to the 1537 ones with  $\log \Delta_{\mathbf{K}} \leq 500$ .

**Final remarks.** In [BDF08, Th. 4.3] the authors prove that for a fixed degree  $T(\mathbf{K}) \gg (\log \Delta_{\mathbf{K}} \log \log \Delta_{\mathbf{K}})^2$  and conjecture that  $T(\mathbf{K}) \sim \frac{1}{16}(\log \Delta_{\mathbf{K}} \log \log \Delta_{\mathbf{K}})^2$  while our computations suggest that  $T_1(\mathbf{K})$  has smaller order. We will prove in a subsequent article [GM15] that  $T(\mathbf{K}) \asymp (\log \Delta_{\mathbf{K}} \log \log \Delta_{\mathbf{K}})^2$  and that  $T_1(\mathbf{K}) \ll (\log \Delta_{\mathbf{K}})^2$ .

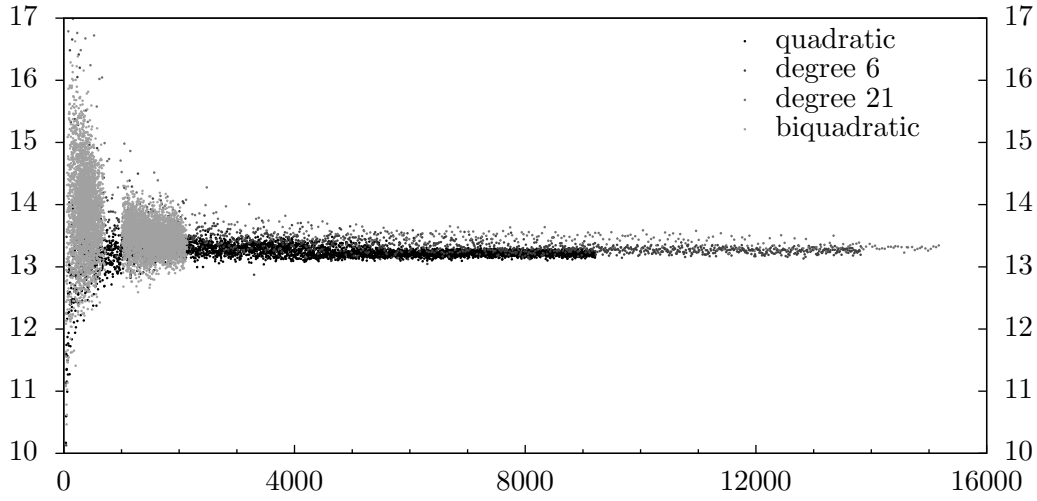


FIGURE 1:  $\frac{T_1(\mathbf{K})}{T(\mathbf{K})}(\log \log \Delta_{\mathbf{K}})^2$  for some pure fields; in abscissa  $\log \Delta_{\mathbf{K}}$ .

**Input:** a number field  $\mathbf{K}$

**Input:** a positive real  $\delta$

**Input:** a positive integer  $N_{\max}$

**Output:** an  $N \leq N_{\max}$  such that  $(N, \delta)$  is  $K$ -good or 0

```

1  $tab \leftarrow (2N_{\max} + 1)$ -dimensional array;
2  $tab[0] \leftarrow 0$ ;
3  $A \leftarrow N_{\max} \times N_{\max}$  identity matrix;
4  $N \leftarrow 0$ ;
5 while  $N < N_{\max}$  do
6    $N \leftarrow N + 1$ ;
7    $tab[2N - 1] \leftarrow (2N - 1)GRHcheck(\mathbf{K}, (2N - 1)\delta)$ ;
8    $tab[2N] \leftarrow 2NGRHcheck(\mathbf{K}, 2N\delta)$ ;
9   for  $i \leftarrow 1$  to  $N$  do
10     $A[N, i] \leftarrow tab[N + i] - tab[N - i]$ ;
11     $A[i, N] \leftarrow A[N, i]$ ;
12  end
13  if  $\det A < 0$  then
14    return  $N$ ;
15  end
16 end
17 return 0;

```

**Function**  $NDelta(\mathbf{K}, \delta, N_{\max})$

**Input:** a number field  $\mathbf{K}$

**Output:** a bound for the norm of a system of generators of  $\mathcal{C}_{\mathbf{K}}$

```

1  $T_0 \leftarrow 4 \left( \log \Delta_{\mathbf{K}} + \log \log \Delta_{\mathbf{K}} - (\gamma + \log 2\pi)n_{\mathbf{K}} + 1 + (n_{\mathbf{K}} + 1) \frac{\log(7 \log \Delta_{\mathbf{K}})}{\log \Delta_{\mathbf{K}}} \right)^2$ ;
2  $T_0 \leftarrow \min(T_0, 4.01 \log^2 \Delta_{\mathbf{K}})$ ;
3  $N \leftarrow 8$ ;  $\delta \leftarrow 0.0625$ ;
4 while  $\text{NDelta}(\mathbf{K}, \delta, N) = 0$  do
5   |  $\delta \leftarrow \delta + 0.0625$ ;
6 end
7  $T_h \leftarrow \text{OptimalT}(\mathbf{K}, N, e^{2N(\delta-0.0625)}, e^{2N\delta})$ ;
8  $T \leftarrow T_h + 1$ ;
9 while  $T_h < T \parallel T > T_0$  do
10  |  $T \leftarrow T_h$ ;  $N \leftarrow 2N$ ;
11  |  $T_h \leftarrow \text{OptimalT}(\mathbf{K}, N, 1, T_h)$ ;
12 end
13 return  $T$ ;

```

**Function** Bound( $\mathbf{K}$ )

#### REFERENCES

- [PARI15] The PARI Group, Bordeaux, *PARI/GP version 2.8*, 1985–2015, available from <http://pari.math.u-bordeaux.fr/>.
- [BDF08] Karim Belabas, Francisco Diaz y Diaz, and Eduardo Friedman, *Small generators of the ideal class group*, Math. Comp. **77** (2008), no. 262, 1185–1197.
- [GM15] Loïc Grenié and Giuseppe Molteni, *Explicit bounds for algorithms computing class field generators*, preprint.

(L. Grenié) DIPARTIMENTO DI INGEGNERIA GESTIONALE, DELL'INFORMAZIONE E DELLA PRODUZIONE, UNIVERSITÀ DI BERGAMO, VIALE MARCONI 5, 24044 DALMINE (BG) ITALY  
*E-mail address:* [loic.grenie@gmail.com](mailto:loic.grenie@gmail.com)

(G. Molteni) DIPARTIMENTO DI MATEMATICA, UNIVERSITÀ DI MILANO, VIA SALDINI 50, 20133 MILANO, ITALY  
*E-mail address:* [giuseppe.molteni1@unimi.it](mailto:giuseppe.molteni1@unimi.it)